FailSafe Booting: A New Paradigm in Embedded Control

Making Internet Connected Equipment Crashproof with FailSafe Boot ROM

What happens when you send a software upgrade to an Internet connected system in the field and there is a hardware or software crash while the download is in process? The software is corrupted and the system cannot re-boot. If the download was being sent to hundreds or even thousands of systems at the same time the result can be catastrophic.

The Difference between the Failsafe and Non-Failsafe Systems

When a watchdog timer scheme other than ZF's FailSafe system reaches a point where it cannot recover a hard reset is performed. If the system SW has been corrupted the system will continuously try to re-boot without success. The system will not come up until it has been repaired. This usually requires sending out a field service technician or sending the equipment in for repair.

With ZF's FailSafe Boot ROM system in a product, if a failure occurs, the system will reach a hard reset, enable the FailSafe mechanism and allow recovery of the software from any of a number of sources (backup chips, dial-out through a modem, etc.). Once the system SW is reloaded the device can re-boot and resume operation.

Protecting your system with the embedded features of the ZF *MachZPCe*™ device can be accomplished simply and reliably. The devices you will use include the dual watchdog timer, the FailSafe Boot ROM, the Z-Tag interface, the bootstrap register and a bit of code. The result will be a system that always boots, can diagnose the failure and always recovers.

Watchdog Timer Role

The watchdog timer checks against possible failures and bugs in the application program or operating system that make the SOC uncontrollable. Both watchdog timers generate events to notify the system of an error condition. These timers are individually initialized to a preset value. After initialization, WD1 begins a countdown that is reset to the initial value by SW writing into the watchdog control register (tickle function) or external HW driving logical "1" to an external control pin. If WD1 reaches zero it indicates that the SW has been unable to reset the timer in the allotted time and an event is generated to take corrective actions or to reset the device.

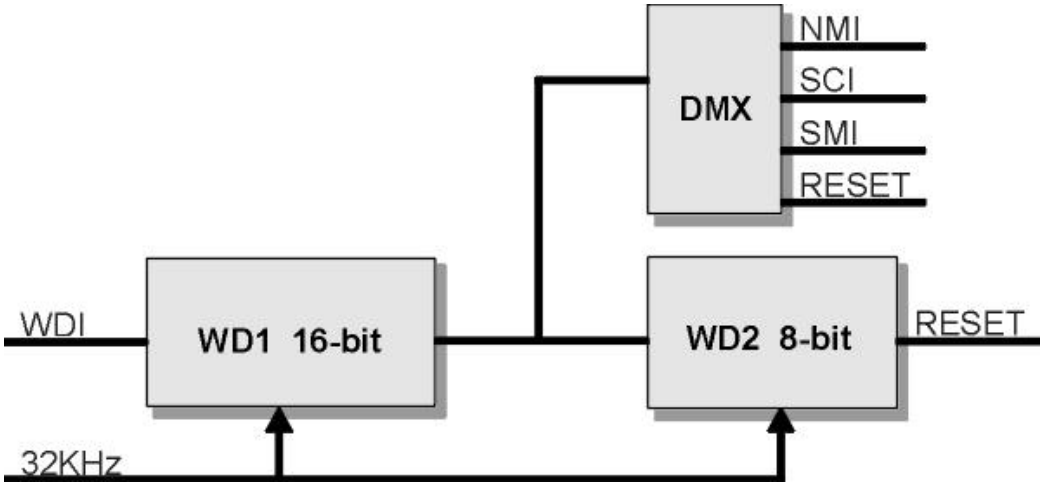

Figure 1: Watchdog Block Diagram

Once the first watchdog timer expires the SW can attempt to gain control of the system using an interrupt handler routine triggered by any of the events connected to the WD1 output line. If the SW is successful, the program can resume as normal. The expired WD1 counter also enables the second watchdog counter (WD2). The second WDT is used to monitor the success of the SW recovery mechanism. If the second timer expires it triggers a HW system reset.

Bootstrap Register Role

A bit on the bootstrap register indicates to the system that a WD timer reset has occurred thereby triggering a FailSafe Boot.

Failsafe Boot Role

The FailSafe Boot ROM is built-in code that initializes the SOC device and uses the Z-Tag interface to load the information it needs to recover the system. This code has multiple features that can allow any designer complete flexibility and control over the system.

Z-Tag Role

The EEPROM containing the SW required to execute the system mandated recovery mechanism (including the contact number for code downloads) is connected to the SOC via the Z-Tag interface. The code in the EEPROM can be as simple as the dial-up instructions for an internet appliance which would allow remote surfing of the device or as complex as a full set of diagnostics and repair programs.